Exercise: Explaining the threat landscape

Case study

The staff at Sam's Scoops are excellent ice cream makers and make a product that is much loved in their seaside community; however, they know little about good online practices. Your task is to gather information on the do's and don'ts of online actions and then share your findings with the team. To be more specific, you'll identify **three vulnerabilities**, and for each one, you'll describe the **risk** it brings, the **type of attack** that a cybercriminal might use to exploit it, and a **mitigation** technique that can be used to reduce risk and improve safety.

Instructions

Step 1: Identify plausible online threats

Identify three potential threats that present a risk to a budding ice cream business looking to establish an online presence. Consider the types of online activities that small businesses tend to engage in. You can review the previous lesson content for ideas but expect to conduct some external research as well.

Step 2: Identify the risks posed by each threat

Once you have figured out the threats, explain how each one can put the company at risk of an attack.

Step 3: Identify attacks used to exploit each threat, and their effects

By which means might an attacker exploit each vulnerability, and how would the company be affected if an attack is carried out?

Step 4: Identify preventative measures relative to each threat that one can take to better protect the business

Make Sam's team aware of what steps they can take to reduce vulnerabilities and better safeguard themselves against risks.

Step 5: Present your findings

Write a summary of what you have found and consult the example below to understand how to format your report. Remember that you are presenting to an audience with limited knowledge of online dangers, so keep it simple and explain all unfamiliar terms. You can also support your explanations with images and diagrams as needed.

Threat #1:

[Vulnerability]: **Account password shared with an acquaintance**
Making a password known to even one person significantly raises the risk of that password ending up in the hands of someone with malicious intent.

[Risk]: **Unintended access**
The password may be used to gain access to an account by someone who isn't meant to have it.

[Attack]: **Theft of sensitive data**
Once unauthorized access has been gained, an individual may acquire sensitive information such as personal and financial details.

[Mitigation]: **Change the password, don't share!**
If a password has been shared, the account password should be changed immediately to render the shared one useless. And make sure no one knows the new password!

Threat #2:

[Vulnerability]: Lack of website security updates
Failing to regularly update the website's software and security patches leaves it exposed to known vulnerabilities that cybercriminals can exploit.

[Risk]: Website defacement and data breaches
Outdated software makes it easier for attackers to deface the website, altering its content to spread malicious messages. Moreover, they can exploit vulnerabilities to gain unauthorized access to customer data.

[Attack]: Injection attacks and defacement
Cybercriminals may use injection attacks, such as SQL injection, to manipulate the website's database and gain administrative privileges, allowing them to deface the site.

[Mitigation]: Regularly update software and use web application firewalls
Frequently update the website's software and apply security patches promptly to address known vulnerabilities. Implementing a web application firewall can also help detect and prevent injection attacks.

Threat #3:

[Vulnerability]: Phishing emails targeting employees
Employees with limited knowledge of online dangers may fall victim to phishing emails, exposing the company to various risks.

[Risk]: Data breaches and financial losses
If an employee unknowingly discloses sensitive information or credentials in response to a phishing email, cybercriminals can gain access to the company's systems and cause data breaches or financial losses.
[Attack]: Phishing attacks
Cybercriminals may send deceptive emails that appear legitimate, tricking employees into clicking malicious links or sharing sensitive information.

[Mitigation]: Employee training and email filtering
Regularly educate employees about phishing risks and the importance of verifying the authenticity of emails. Implement email filtering solutions to identify and block phishing emails before they reach employees' inboxes.

Conclusion:

In conclusion, as Sam's Scoops looks to establish an online presence, it must be aware of potential threats that could compromise its operations and reputation. By addressing vulnerabilities proactively and implementing appropriate mitigation measures, such as changing passwords, keeping software up to date, and providing employee training, the company can significantly improve its online safety.

Remember, maintaining a secure online presence is an ongoing process, and continuous vigilance is key to safeguarding against cyber threats.